AMENDMENTS TO THE SPECIFICATION:

Please amend the specification as follows:

Page 32, replace the paragraph beginning at line 3 with the following paragraph:

a1

According to the crypto processing apparatus of this embodiment, an LSI having abundant functions capable of handling the finite field GF(2^m) based elliptic curve cryptosystem as well as the integer based ~~RAS~~ RSA system can be provided as a crypto processing coprocessor without specifically increasing the packing area. An encryption/decryption apparatus capable of handling both ~~RAS~~ RSA and elliptic curve cryptosystem can be implemented in even an apparatus having a small packing area, such as an IC card.

Page 35, replace the paragraph beginning at line 12, with the following paragraph:

a2

In this embodiment, the full adder shown in FIG. 5 is used as the full adder 42 having the carry control function. However, the full adder 43 or 44 having a carry control function shown in FIG. 6 or 7 may be used ~~in stead~~ instead of the full adder 42 having a carry control function.

Page 35, replace the paragraph beginning at line 24, with the following paragraph:

a3

This embodiment is a concrete example of the modulo section of the first embodiment. As shown in FIG. 10, a controller unit 5 includes a finite field GF(2^m) arithmetic controller ~~22a~~ 22 having a modulo function added to the above function, and a3

a quotient acquisition circuit 50 which is controlled by the modulo function and has an inverse calculator section 51.

Page 36, replace the paragraph beginning at line 4, with the following paragraph:

a4

In this case, in addition to the above function of controlling an arithmetic unit 4 to obtain a multiply result of c'(x) of equation (5), the finite field GF(2^m) arithmetic controller ~~22a~~ 22 has the function of controlling the arithmetic unit 4 and quotient acquisition circuit 50 to execute a modulo for this multiply result c'(x) using a modulo polynomial f(x). More specifically, the control function includes the function of inputting/outputting data to/from a memory 2 and buffers 17X, 17Y, 17Z, and 17R on the basis of the operation algorithm to be described later, and the function o generating various commands such as a multiply command, addition command, and inverse operation command and supplying them to corresponding arithmetic circuits in accordance with the input/output operation.

Page 36, replace the paragraph beginning at line 37, with the following paragraph:

a5

More specifically, the quotient acquisition circuit 50 is controlled by the finite field GF(2^m) arithmetic controller ~~22a~~ 22, and has the function of supplying the upper two blocks ($F_{L-1(x)}$, $F_{L-2(x)}$) of the modulo polynomial f(x) in the memory 2 to the inverse calculator section 51 in only one time of the modulo and making the section 51 calculate the inverse β(x) of the upper two blocks, the function of reading out the obtained inverse β(x) from the memory 2 when the inverse is written in the memory 2, the function of obtaining a quotient γ(x) by multiplying the readout inverse β(x) and the upper two blocks ($C'_{L-1(x)}$, $C'_{L-2(x)}$) of the current dividend polynomial, the function of setting the obtained quotient γ(x) as a quotient qi(x) of the upper two blocks and writing the quotient qi(x) in the memory 2, and the function of repeating the operation from reading out the inverse β(x) to writing the quotient qi(x) until a residue c(x) is obtained, as shown in FIG. 11.

a^5

Page 41, replace the paragraph beginning at line 20, with the following paragraph:

After setting the upper two blocks ($F_{L-1(x)}$, $F_{L-2(x)}$) as a divisor in a coefficient unit 93 in FIG. 27, the inverse calculator section 51 inputs the dividend ~~x^{2i}~~ x^{2k} to the shift register from higher orders and repeats a shift in units of clocks 2*16 times, thereby obtaining a 32-bit inverse α(x). Note that one block may consist of 8 or 32 bits or another arbitrary number of bits. In such a case as well, the inverse α(x) can be calculated by the same scheme.

a^6